Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1–10. (Canceled).

11. (Currently Amended) A method for controlling access to network resources, comprising:

at a central configuration machine:

defining an internal protection domain for each of a plurality of firewalls, each internal protection domain including at least one zone, each zone having at least one access-controlled network resource ;

defining at least one external protection domain for the plurality of firewalls, the external protection domain including at least one zone having at least one access-controlled network resource, wherein each of the plurality of firewalls protects the internal protection domain relative to the external protection domain and each of the internal and external protection domains comprise one or more of networks and subnetworks of machines;

creating a plurality of resource groups, each resource group including at least one zone;

specifying an access control rule, including a scope, for each resource group, the scope, and thus the access control rule, is capable of being interpreted by each of the

plurality of firewalls differently depending on the value of the scope and network resource characteristics associated with each of the plurality of firewalls;

configuring each firewall using the access control rules; and

at each firewall:

in response to a request to access a destination network resource received from a source network resource, determining whether to apply the access control rule specified for the resource group associated with the destination network resource based on the scope of the access control rule.

12. (Previously Presented) A method according to claim 11, further comprising:

determining the protection domain of the access-controlled network resources using firewall network interfaces through which communications pass to reach said access-controlled network resources.

13. (Previously Presented) A method according to claim 12, further comprising:

associating each firewall network interface with an internal or external protection domain,

determining incoming and outgoing firewall network interfaces of current traffic,

analyzing whether the incoming and outgoing firewall network interfaces are attached to an internal or external protection domain, and

applying the rule for controlling access only if the incoming and outgoing firewall network interfaces are attached to the same internal protection domain and the access-controlled network resources belong to the same protection domain.

14. (Previously Presented) A method according to claim 11, wherein the rule for controlling access is applied between each of the access-controlled network resources of a source resource group and a destination resource group.

15. (Previously Presented) A method according to claim 12, wherein the rule for controlling access is applied between each of the access-controlled network resources of a source resource group and a destination resource group.

16. (Previously Presented) A method according to claim 13, wherein the rule for controlling access is applied between each of the access-controlled network resources of a source resource group and a destination resource group.

17. (Previously Presented) A method according to claim 11, further comprising:

specifying the scope of each rule for controlling access as local or global,

when the scope of the rule is local, applying the rule to the access-controlled network resources in question only if said access-controlled network resources belong to the same internal or external protection domain, and

when the scope of the rule is global, applying the rule to all of the access-controlled network resources in question.

18. (Previously Presented) A method according to claim 12, further comprising:

specifying the scope of each rule for controlling access as local or global,

when the scope of the rule is local, applying the rule to the access-controlled network resources in question only if said access-controlled network resources belong to the same internal or external protection domain, and

when the scope of the rule is global, applying the rule to all of the access-controlled network resources in question.

19. (Previously Presented) A method according to claim 13, further comprising:

specifying the scope of each rule for controlling access as local or global,

when the scope of the rule is local, applying the rule to the access-controlled network resources in question only if said access-controlled network resources belong to the same internal or external protection domain, and

when the scope of the rule is global, applying the rule to all of the access-controlled network resources in question.

20. (Previously Presented) A method according to claim 14, further comprising:

specifying the scope of each rule for controlling access as local or global,

when the scope of the rule is local, applying the rule to the access-controlled network resources in question only if said access-controlled network resources belong to the same internal or external protection domain, and

when the scope of the rule is global, applying the rule to all of the access-controlled network resources in question.

21. (Previously Presented) A method according to claim 15, further comprising:

specifying the scope of each rule for controlling access as local or global,

when the scope of the rule is local, applying the rule to the access-controlled network resources in question only if said access-controlled network resources belong to the same internal or external protection domain, and

when the scope of the rule is global, applying the rule to all of the access-controlled network resources in question.

22. (Previously Presented) A method according to claim 16, further comprising:

specifying the scope of each rule for controlling access as local or global,

when the scope of the rule is local, applying the rule to the access-controlled network resources in question only if said access-controlled network resources belong to the same internal or external protection domain, and

when the scope of the rule is global, applying the rule to all of the access-controlled network resources in question.

23. (Currently Amended) A system for controlling access to network resources, comprising:

an external network including at least one external subnetwork having at least one network resource;

a plurality of firewalls, coupled to the external network, each firewall including at least one internal subnetwork, each internal subnetwork having at least one access-controlled network resource; and

a central configuration machine, coupled to the external network, adaptively configured to:

define an internal protection domain for each of the plurality of firewalls, each internal protection domain including a zone corresponding to each internal subnetwork,

define an external protection domain for the plurality of firewalls, the external protection domain including a zone corresponding to each external subnetwork, wherein each of the plurality of firewalls protects the internal protection domain relative to the external protection domain and each of the internal and external protection domains comprise one or more of networks and subnetworks of machines,

create a plurality of resource groups, each resource group including at least one zone,

specify an access control rule, including a scope, for each resource group, the scope, and thus the access control rule, is capable of being interpreted by each of the plurality of firewalls differently depending on the value of the scope and network resource characteristics associated with each of the plurality of firewalls, and

configure each firewall using the access control rules.

24. (Previously Presented) A device according to claim 23, wherein the central configuration machine includes a graphical interface from which an administrator can enter the protection domains and the access control rules.

25. (Canceled).

26. (Previously Presented) A device according to claim 24, wherein the graphical interface allows the administrator to define a local or global scope for the access control rule.